UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE IPHONE APPLICATION LITIG.	Case No.: 11-MD-02250-LHK ORDER GRANTING IN PART AND DENYING IN PART DEFENDANTS' MOTIONS TO DISMISS

A putative nationwide class of plaintiffs bring suit against Apple, Inc., Admob, Inc., Flurry, Inc., AdMarval, Inc., Google, Inc., and Medialets, Inc., (aside from Apple, collectively "Mobile Industry Defendants"[1]) for alleged violations of federal and state law. Plaintiffs are United States' residents who use mobile devices manufactured by Apple that operate Apple's "iOS" proprietary operating systems, or what Plaintiffs refer to as iDevices (e.g., iPhone, iPad, and iPod Touch). Plaintiffs claim that Defendants violated their privacy rights by unlawfully allowing third party applications ("apps") that run on the iDevices to collect and make use of, for commercial purposes, personal information without user consent or knowledge. Apple and the Mobile Industry Defendants have each filed motions to dismiss on various grounds, including lack of Article III standing, consent to privacy agreements, and additional claim-specific reasons. A hearing was held on May 3, 2012. For the reasons explained below, the Court GRANTS Defendant Mobile Industry Defendants motion to dismiss and GRANTS in part and DENIES in part Apple's motion to

[1] Mobile Industry Defendants are referred to by the Plaintiffs as the "Tracking Defendants."

dismiss. Specifically, Plaintiffs' claims against the Mobile Industry Defendants for violations of the Stored Communications Act, violations of the California Constitutional right to privacy, violations of the Computer Fraud and Abuse Act, trespass, conversion, and unjust enrichment are dismissed. Plaintiffs' claims against Apple for violations of the Stored Communications Act, violations of the Wiretap Act, violations of the California Constitutional right to privacy, negligence, violations of the Computer Fraud and Abuse Act, trespass, conversion, and unjust enrichment are dismissed. For the reasons set forth in Section III.D., these claims are dismissed with prejudice. Plaintiffs' claims against Apple for violations of the Consumer Legal Remedies Act and the Unfair Competition Law survive Apple's motion to dismiss.

I. BACKROUND

A. Factual Background

Unless otherwise noted, the following allegations are taken from the Amended Consolidated Complaint and are presumed to be true for purposes of ruling upon Defendants' motions to dismiss. Generally speaking, Plaintiffs' Amended Consolidated Complaint asserts claims with respect to two separate putative classes of individuals and challenges two separate aspects of the iDevices used by Plaintiffs.

The iDevice Class[2]

iDevices enable users to download apps via Apple's "App Store" application and website. First Amended Consolidated Complaint ("AC") ¶ 86. Apple exercises significant control over the apps that are available in its store. *Id.* ¶¶ 123-126. Apple's App Store has set Apple products apart from Apple's competitors: "[i]n the post 3G 2.0 iOS era, the success of Apple's iPhones sales [sic] is inextricably linked to consumers' access to its App Store." *Id.* ¶ 86. Apple represents to users of the App Store that it "takes precautions—including administrative, technical, and physical measures—to safeguard your personal information against theft, loss, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction." *Id.* ¶ 78.

[2] The Court refers to the "iDevice Class" and the "Geolocation Class" even though these classes have not been certified pursuant to Federal Rule of Civil Procedure 23. Any reference to "classes" within this Order is merely for ease of discussion and is not intended to imply a position regarding whether either class would be certifiable under the federal rules.

Although the apps at issue in this litigation are provided for free, Plaintiffs contend that they in fact pay a price for the use of the "free" apps because these Apple-approved apps allow their personal data to be collected from their iDevices. AC ¶¶ 1; 160. Plaintiffs allege that Apple designs its mobile devices to allow personal information to be disclosed to the Mobile Industry Defendants. *Id.* ¶¶ 159-60. "When users download and install the Apps on their iDevices the [Mobile Industry Defendants'] software accesses personal information on those devices without users' awareness or permission and transmits the information to the [Mobile Industry Defendants]." *Id.* ¶ 161. The information collected by Defendants includes Plaintiffs' addresses and current whereabouts; the unique device identifier ("UDID") assigned to the iDevice; the user's gender, age, zip code and time zone; and app-specific information such as which functions Plaintiff performed on the app. *Id.* ¶ 2; *see also id.* ¶¶ 53-67, 161. These practices have allowed the Mobile Industry Defendants to "acquire details about consumers and to track consumers on an ongoing basis, across numerous applications and tracking consumers when they accessed Apps from different mobile devices." *Id.* ¶ 164.

Plaintiffs allege that, in light of Apple's public statements about protecting user privacy, Plaintiffs did not expect or consent to the Mobile Industry Defendants' tracking and collecting their app use or otherwise personal information. *Id.* ¶ 173-74. Moreover, Plaintiffs allege that they consider the information about their mobile communications to be personal and confidential. *Id.* ¶ 177.

Plaintiffs assert that these practices have led to several concrete harms to the "iDevice Class," defined as "[a]ll persons residing in the United States who have purchased iPhones and downloaded free Apps from the App Store on a mobile device that runs Apple's iOS, from December 1, 2008 to the date of the filing of this Complaint." AC ¶ 203. For one, the Mobile Industry Defendants' actions have consumed finite resources in the form of bandwidth and storage space on their iDevices. *Id.* ¶ 198. For example, downloading the Weather Channel App "caused a compressed .zip file of approximately two megabytes in size to be downloaded to each of Plaintiffs' iDevices and for purposes unrelated to those expected in the Weather Channel App." *Id.* Additionally, the transmission of personal information to the Mobile Industry Defendants was done

without encryption, thus "exposing each Plaintiff to unreasonable risks of the interception of their personal information ." *Id.* ¶¶ 66-67. Finally, Plaintiffs allege that as a result of Apple's failure to disclose its practices with respect to the allegedly "free apps," Plaintiffs overpaid for their iDevices. In other words "[h]ad Apple disclosed the true cost of the purportedly free Apps . . . the value of the iPhones would have been materially less than what Plaintiffs paid." *Id.* ¶ 29.

The Geolocation Class

Additionally, Plaintiffs Gupta and Rodimer represent the "Geolocation Class," a putative class of iDevice purchasers who "have unwittingly, and without notice or consent transmitted location data to Apple's servers." *Id.* ¶ 204. Apple designed its iOS 4 software to retrieve and transmit geolocation information located on its customers' iPhones to Apple's servers. *Id.* ¶ 30. Plaintiffs allege that in June 2010, with the release of its iOS 4 operating system, Apple began intentionally collecting Plaintiffs' precise geographic location and storing that information on the iDevice in order to develop an expansive database of information about the geographic location of cellular towers and wireless networks throughout the United States. *Id.* ¶¶ 115, 137. The geographic location information was accumulated from either Wi-fi towers or cell phone towers, and in some cases from the GPS data on Plaintiffs' devices. *Id.* ¶ 115. Apple represented that users could prevent Apple from collecting geolocation data about them by switching the Location Services setting on their iDevices to "off." *Id.* ¶ 31. Plaintiffs contend that Apple continued to monitor and store information about Plaintiffs locations even when the functionality was disabled on users' iDevices. *Id.* ¶¶ 32, 141. Plaintiffs contend that had Apple "disclosed the true cost of the . . . geolocation features, the value of the iPhones would have been materially less than what Plaintiffs paid." *Id.* ¶ 29. Moreover, Plaintiffs allege that the storage of the location histories on their iDevices consume valuable memory space. *Id.* ¶ 119-121.

B. Procedural History

This case is a consolidated multi-district litigation involving nineteen putative class action lawsuits. *See generally* First Consolidated Class Action Complaint ("Consolidated Complaint"), 10-cv-05878-LHK, ECF No. 71. The first two of these consolidated actions were filed on December 23, 2010. *See Lalo v. Apple, Inc.*, et al., 10-cv-05878-LHK (the "Lalo Action") and

Freeman v. Apple, Inc., et al., 10-cv05881-LHK (the "Freeman Action"). Other actions in this District and throughout the country have followed. These other actions, filed throughout the country, involve substantially similar allegations against Apple and other Defendants. On August 25, 2011, the Judicial Panel on Multidistrict Litigation ("MDL Panel") issued a Transfer Order, centralizing these actions in the Northern District of California before the undersigned. *See* August 25, 2011 Transfer Order in MDL No. 2250, ECF No. 1.

The First Consolidated Complaint was filed on April 21, 2011. The Consolidated Complaint contained eight claims: (1) Negligence against Apple only; (2) Violation of Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030; (3) Computer Crime Law, Cal. Penal Code § 502; (4) Trespass on Chattel; (5) Consumer Legal Remedies Act ("CLRA"), Cal. Civ. Code § 1750 against Apple only; (6) Unfair Competition under Cal. Bus. & Prof. Code § 17200; (7) Breach of Covenant of Good Faith and Fair Dealing; and (8) Unjust Enrichment. Defendant Apple filed a motion to dismiss the First Consolidated Complaint on June 20, 2011. *Lalo Action*, ECF No. 142. The Mobile Industry Defendants also filed a motion to dismiss on the same day. *Lalo Action*, ECF No. 145. Plaintiffs' opposition was filed on July 18, 2011. *Lalo Action*, ECF No. 153. Replies were filed on August 3, 2011. *Lalo Action*, ECF Nos. 159, 160.

On September 20, 2011, the Court granted Defendants' motions to dismiss on the basis that Plaintiffs failed to establish Article III Standing. *See generally* September 20, 2011 Order Granting Motions to Dismiss for Lack of Article III Standing ("September 20 Order"), ECF No. 8. Specifically, the Court found that "[d]espite a lengthy Consolidated Complaint, Plaintiffs do not allege injury in fact *to themselves*;" and that Plaintiffs failed to differentiate amongst the Mobile Industry Defendants. September 20 Order at 6. Alternatively, the Court identified deficiencies with respect to each of Plaintiffs' eight causes of action in the Consolidated Complaint. September 20 Order at 13-21. Plaintiffs were given leave to amend the complaint and were instructed that "[a]ny amended complaint must remedy the deficiencies identified," in the Order. *Id.* at 21.

On November 22, 2011, Plaintiffs' filed the First Amended Consolidated Class Action Complaint ("Amended Consolidated Complaint" or "AC"). ECF No. 25. The Amended Consolidated Complaint contains thirteen causes of action: (1) Violation of the Stored

Communications Act ("SCA"), 18 U.S.C. § 2701, *et seq.*, on behalf of the Geolocation Class against Apple only; (2) Violation of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510, *et seq.*, on behalf of the Geolocation Class against Apple only; (3) Violation of the California Constitution Art. I, Section 1 on behalf of the Geolocation Class against Apple only; (4) Violation of the California Constitution Art. I, Section 1 on behalf of the iDevice Class against all Defendants; (5) Negligence against Apple only; (6) Violation of Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, on behalf of the Geolocation Class against Apple only; (7) Violation of the CFAA, on behalf of the iDevice Class against all Defendants; (8) Trespass against all Defendants; (9) Violation of the Consumer Legal Remedies Act ("CLRA"), Cal. Civ. Code § 1750 against Apple only; (10) Violation of the Unfair Competition under Cal. Bus. & Prof. Code § 17200, against Apple only; (11) Violation of the SCA on behalf of the iDevice Class against the Tracking Defendants;[3] (12) Conversion on behalf of the iDevice Class against all Defendants; and (13) Assumpsit and Restitution on behalf of the iDevice Class against all Defendants. On January 10, 2012, Defendants filed the pending motions to dismiss. *See* ECF Nos. 42, 43. Plaintiffs filed an opposition to Defendants' motions on March 8, 2012. ECF No. 51. Defendants filed replies on April 5, 2012. ECF Nos. 54, 55. A hearing was held on May 3, 2012. Defendants argue that Plaintiffs' lack Article III standing and that alternatively, the Amended Consolidated Complaint fails to state a claim upon which relief can be granted as to each of the thirteen causes of action pled.

II. LEGAL STANDARD

A. Motion to Dismiss Under Rule 12(b)(1)

A jurisdictional challenge may be facial or factual. *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). Where the attack is facial, the court determines whether the allegations contained in the complaint are sufficient on their face to invoke federal jurisdiction, accepting all material allegations in the complaint as true and construing them in favor of the party

[3] Originally this claim was brought against all Defendants, but Plaintiffs clarified in their Opposition to Defendants' Motions to Dismiss ("Opp'n") that Count Eleven was withdrawn as to Defendant Apple, and was only being asserted as to the Tracking Defendants. *See* Opp'n at 33 n.30.

asserting jurisdiction. *See Warth v. Seldin*, 422 U.S. 490, 501 (1975). Where the attack is factual, however, "the court need not presume the truthfulness of the plaintiff's allegations." *Safe Air for Everyone*, 373 F.3d at 1039. In resolving a factual dispute as to the existence of subject matter jurisdiction, a court may review extrinsic evidence beyond the complaint without converting a motion to dismiss into one for summary judgment. *See id.*; *McCarthy v. United States*, 850 F.2d 558, 560 (9th Cir.1988) (holding that a court "may review any evidence, such as affidavits and testimony, to resolve factual disputes concerning the existence of jurisdiction"). Once a party has moved to dismiss for lack of subject matter jurisdiction under Rule 12(b)(1), the opposing party bears the burden of establishing the Court's jurisdiction. *See Kokkonen v. Guardian Life Ins. Co.*, 511 U.S. 375, 377 (1994); *Chandler v. State Farm Mut. Auto. Ins. Co.*, 598 F.3d 1115, 1122 (9th Cir. 2010).

B. Motion to Dismiss Under Rule 12(b)(6)

A motion to dismiss pursuant to Rule 12(b)(6) for failure to state a claim upon which relief can be granted "tests the legal sufficiency of a claim." *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001). Dismissal under Rule 12(b)(6) may be based on either (1) the "lack of a cognizable legal theory," or (2) "the absence of sufficient facts alleged under a cognizable legal theory." *Balistreri v. Pacifica Police Dep't*, 901 F.2d 696, 699 (9th Cir. 1990). While "'detailed factual allegations'" are not required, a complaint must include sufficient facts to "'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 129 S.Ct. 1937, 1949 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.*

For purposes of ruling on a Rule 12(b)(6) motion to dismiss, the Court accepts all allegations of material fact as true and construes the pleadings in the light most favorable to the plaintiffs. *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). The Court need not, however, accept as true pleadings that are no more than legal conclusions or the "'formulaic recitation of the elements' of a cause of action." *Iqbal*, 129 S.Ct. at 1949 (quoting *Twombly*, 550 U.S. at 555). Mere "conclusory allegations of law and unwarranted inferences are

insufficient to defeat a motion to dismiss for failure to state a claim." *Epstein v. Wash. Energy Co.*, 83 F.3d 1136, 1140 (9th Cir. 1996); *accord Iqbal*, 129 S. Ct. at 1949–50.

C. Leave to Amend

Under Rule 15(a) of the Federal Rules of Civil Procedure, leave to amend "shall be freely given when justice so requires," bearing in mind "the underlying purpose of Rule 15 to facilitate decision on the merits, rather than on the pleadings or technicalities." *Lopez v. Smith*, 203 F.3d 1122, 1127, 1140 (9th Cir. 2000) (en banc) (internal quotation marks and alterations omitted). When dismissing a complaint for failure to state a claim, "'a district court should grant leave to amend even if no request to amend the pleading was made, unless it determines that the pleading could not possibly be cured by the allegation of other facts.'" *Id.* at 1127 (quoting *Doe v. United States*, 58 F.3d 494, 497 (9th Cir. 1995)). Generally, leave to amend shall be denied only if allowing amendment would unduly prejudice the opposing party, cause undue delay, or be futile, or if the moving party has acted in bad faith. *Leadsinger, Inc. v. BMG Music Publ'g.*, 512 F.3d 522, 532 (9th Cir. 2008).

III. ANALYSIS

A. Article III Standing

An Article III federal court must ask whether a plaintiff has suffered sufficient injury to satisfy the "case or controversy" requirement of Article III of the U.S. Constitution. To satisfy Article III standing, plaintiff must allege: (1) injury-in-fact that is concrete and particularized, as well as actual and imminent; (2) wherein injury is fairly traceable to the challenged action of the defendant; and (3) it is likely (not merely speculative) that injury will be redressed by a favorable decision. *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000); *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561-62 (1992). A suit brought by a plaintiff without Article III standing is not a "case or controversy," and an Article III federal court therefore lacks subject matter jurisdiction over the suit. *Steel Co. v. Citizens for a Better Environment*, 523 U.S. 83, 101 (1998). In that event, the suit should be dismissed under Rule 12(b)(1). *See id.* at 109-110.

Because "injury" is a requirement under both Article III and Plaintiffs' individual causes of action, the Court notes at the outset that "the threshold question of whether [Plaintiffs have] standing (and the [C]ourt has jurisdiction) is distinct from the merits of [Plaintiffs'] claim." *Maya v. Centex Corp.*, 658 F.3d 1060, 1068 (9th Cir. 2011). Standing "in no way depends on the merits of the plaintiff's contention that particular conduct is illegal." *Warth*, 422 U.S. at 500; *accord Equity Lifestyle Props., Inc. v. Cnty. of San Luis Obispo*, 548 F.3d 1184, 1189 n.10 (9th Cir. 2008) ("The jurisdictional question of standing precedes, and does not require, analysis of the merits."). In other words "[a] plaintiff may satisfy the injury-in-fact requirements to have standing under Article III, and thus may be able to 'bring a civil action without suffering dismissal for want of standing to sue,' without being able to assert a cause of action successfully." *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 712 n.5 (N.D. Cal. 2011) (citing *Doe v. Chao*, 540 U.S. 614, 624-25 (2004)). Defendants argued in their briefing and at the hearing that Plaintiffs continue to rely on a faulty theory of injury and thus have failed to establish injury in fact that is fairly traceable to the Defendants such that Article III standing has been established. The Court disagrees.

1. Injury In Fact

Plaintiffs' initial complaint relied heavily upon a theory that collection of personal information itself created a particularized injury for the purposes of Article III standing. Relying on *LaCourt v. Specific Media, Inc.*, 2011 U.S. Dist. LEXIS 50543, at *7-13 (C.D. Cal. Apr. 28, 2011), *In re Doubleclick, Inc., Privacy Litig.*, 154 F. Supp. 2d 497, 525 (S.D.N.Y. 2001), and *In re JetBlue Airways Corp., Privacy Litig.*, 379 F. Supp. 2d 299, 327 (E.D.N.Y. 2005), the Court found that Plaintiffs had "not identified an actual injury to themselves," and that "any amended complaint must provide specific allegations with respect to the causal connection between the exact harm alleged (whatever it is) and each Defendants' conduct or role in that harm." September 20 Order at 7 & 9. Additionally, the Court identified the following deficiencies in Plaintiffs' original complaint with respect to the threshold inquiry regarding whether Plaintiffs have established Article III standing: (a) which "iDevices they used;" (b) "which Defendant (if any) accessed or tracked their personal information;" (c) which apps they downloaded that "access[ed]/track[ed]

their personal information," and; (d) "what harm (if any) resulted from the access or tracking of their personal information." September 20 Order at 6.

In contrast to the First Consolidated Complaint, Plaintiffs' allegations in the Amended Consolidated Complaint have been significantly developed to allege particularized injury to the Plaintiffs in this case. For one, Plaintiffs have articulated additional theories of harm beyond their theoretical allegations that personal information has independent economic value. In particular, Plaintiffs have alleged actual injury, including: diminished and consumed iDevice resources, such as storage, battery life, and bandwidth (AC ¶¶ 3, 63b, 72d, 198); increased, unexpected, and unreasonable risk to the security of sensitive personal information (AC ¶¶ 4, 18, 66-67); and detrimental reliance on Apple's representations regarding the privacy protection afforded to users of iDevice apps (AC ¶¶ 72c, 80-82).

Additionally, Plaintiffs have addressed the deficiencies identified in the Court's September 20 Order. Specifically, in the Amended Consolidated Complaint, Plaintiffs describe: (a) the specific iDevices used (*see, e.g.*, AC ¶¶ 64a-g); (b) which Defendants accessed or tracked their personal information (*see, e.g.*, AC ¶¶ 56-63); (c) which apps they downloaded that accessed or tracked their personal information (*see, e.g.*, AC ¶¶ 58-60); and (d) what harm resulted from the access or tracking of their personal information (*see, e.g.*, AC ¶¶ 3-4, 18, 63b, 66-67, 72d, 80-82, 198). Plaintiffs have also identified the specific type of personal information collected, such as Plaintiffs' home and workplace locations, gender, age, zip code, terms searched, Plaintiff's app ID and password for specific app accounts, etc., through each of the downloaded apps. *See, e.g.*, AC ¶¶ 58-64. Thus, Plaintiffs have addressed the concerns identified in the Court's September 20 Order and have articulated a particularized harm as to themselves.

Moreover, Plaintiffs also have identified an additional basis for establishing Article III standing. The injury required by Article III may exist by virtue of "statutes creating legal rights, the invasion of which creates standing." *See Edwards v. First Am. Corp.*, 610 F.3d 514, 517 (9th Cir. 2010) (quoting *Warth v. Seldin*, 422 U.S. 490, 500 (1975)). In such cases, the "standing question . . . is whether the constitutional or statutory provision on which the claim rests properly

can be understood as granting persons in the plaintiff's position a right to judicial relief." *Id.* (quoting *Warth*, 422 U.S. at 500)).

In this case, Plaintiffs have alleged a violation of their statutory rights under the Wiretap Act, 18 U.S.C. §§ 2510, *et seq*., against Apple, as well as the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq*., against the Mobile Industry Defendants. AC ¶¶ 219-233; 342-347. The Wiretap Act provides that any person whose electronic communication is "intercepted, disclosed, or intentionally used" in violation of the Act may in a civil action recover from the entity which engaged in that violation. 18 U.S.C. § 2520(a). Similarly, the Stored Communications Act generally prohibits (1) intentionally accessing without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeding authorization to access that facility; and obtaining, altering, or preventing authorized access to a wire or electronic communication while it is in electronic storage. 18 U.S.C. § (a)(1)-(2).

Other courts in this district have recognized that a violation of the Wiretap Act or the Stored Communications Act may serve as a concrete injury for the purposes of Article III injury analysis. *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 711-12 (N.D. Cal.) ("the Court finds that Plaintiffs allege a violation of their statutory rights under the Wiretap Act, 18 U.S.C. §§ 2510, et seq. The Wiretap Act provides that any person whose electronic communication is 'intercepted, disclosed, or intentionally used' in violation of the Act may in a civil action recover from the entity which engaged in that violation. 18 U.S.C. § 2520(a). Thus, the Court finds that Plaintiffs have alleged facts sufficient to establish that they have suffered the injury required for standing under Article III."); *Gaos v. Google, Inc.*, 2012 WL 109446, at *3 (N.D. Cal. Mar. 29, 2012) ("Thus, a violation of one's statutory rights under the SCA is a concrete injury."). Thus, the Court finds that Plaintiffs have established injury in fact for the purposes of Article III standing.

2. Causation: Fairly Traceable to Actions of Defendants

Defendants argue that Plaintiffs have also failed to allege any injury fairly traceable to Apple or to the Mobile Industry Defendants. *See* Apple's Mot. to Dismiss at 10-11; Mobile Industry Defs' Mot. to Dismiss at 16. The allegations in the Amended Consolidated Complaint assert conduct by Defendants which directly or indirectly led to the alleged harm. *See Warth*, 422

U.S. at 504-05 ("The fact that the harm to petitioners may have resulted indirectly does not in itself preclude standing."). As to the Geolocation Class, Plaintiffs assert that Apple designed its iOS 4 software to retrieve and transmit geolocation information located on its customers' iPhones to Apple's servers, that Apple intentionally collected and stored Plaintiffs' precise geographic location, and that this led to loss of storage space on their iDevices and a product that was devalued because it did not perform as promised to consumers. Thus, the alleged harm to the Geolocation Class is fairly traceable to Apple's conduct.

Similarly, Plaintiffs have alleged harm to the iDevice Class that is fairly traceable to both Apple and the Mobile Industry Defendants. Plaintiffs allege that Apple designed its products and the App Store to allow individuals to download third party apps. Additionally, in order to encourage consumers to download apps, Apple represents to users of the App Store that it "takes precautions—including administrative, technical, and physical measures—to safeguard your personal information against theft, loss, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction." *Id.* at ¶ 78. Plaintiffs also allege that the Mobile Industry Defendants' software accesses personal information on those devices without users' awareness or permission and transmits the information to the Mobile Industry Defendants. Moreover, Apple has designed its products to allow consumers' personal information to be transmitted to third parties, such as the Mobile Industry Defendants. According to Plaintiffs, this transfer has led to the consumption of bandwidth and storage space on their iDevices and has led them to overpay for their devices. Thus, as a matter of pleading Article III standing, Plaintiffs have sufficiently articulated the alleged injury is fairly traceable to the conduct of both Defendants. *See Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 1001 (N.D. Cal. 2006) (finding that plaintiffs had standing where the allegations were that AT&T actively partnered to intercept and monitor customer phone lines). Plaintiffs have established that this Court has subject matter jurisdiction over the instant dispute. Accordingly, Defendants' motions to dismiss the Amended Consolidated Complaint pursuant to 12(b)(1) are DENIED.

B. Rule 12(b)(6) Motion to Dismiss Causes of Action

In light of the Court's finding that Plaintiffs have established Article III standing, the Court will turn to whether Plaintiffs have plausibly stated a claim as to each cause of action alleged in the Amended Consolidated Complaint.

1. Stored Communications Act

Plaintiffs' first claim, brought by Plaintiffs Gupta and Rodimer on behalf of the Geolocation Class solely against Apple, is that Apple's conduct violated the federal Stored Communications Act, 18 U.S.C. § 2701, et seq. ("SCA"). AC ¶¶ 224-25. Plaintiffs bring a separate claim under the SCA on behalf of the iDevice Class against all Mobile Industry Defendants.[4] AC ¶ 347.

Enacted in 1986 as Section II of the Electronic Communications Protection Act ("ECPA"), the SCA creates criminal and civil liability for certain unauthorized access to stored communications and records. *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002). The SCA creates a private right of action against anyone who "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C § 2701(a); see id. § 2707 (creating a private right of action). The general prohibitions under § 2701(a), however, do not apply "to conduct authorized (1) by the person or entity providing a wire or electronic communications service; [or] (2) by a user of that service with respect to a communication of or intended for that user." 18 U.S.C. § 2701(c).

Plaintiffs Gupta and Rodimer assert that Apple violated §§ 2701(a)(1) and (a)(2) by intentionally accessing and collecting temporarily stored location data from Geolocation Class members' iPhones after Locations Services was turned "off." AC ¶¶ 224-25. Plaintiffs further assert that the Mobile Industry Defendants violated § 2701(a)(1) by intentionally accessing

[4] The Mobile Industry Defendants also argue that Plaintiffs lack prudential standing to bring an SCA claim. Mobile Industry MTD at 17. Because the Court finds, on other grounds, that Plaintiffs have failed to state a claim for relief under the SCA, the Court need not address this argument. *See Indep. Living Ctr. of S. Cal., Inc. v. Shewry*, 543 F.3d 1050, 1065 n.17 (9th Cir. 2008) ("Unlike the Article III standing inquiry, whether [Plaintiff] maintains prudential standing is not a jurisdictional limitation.") (citations omitted).

electronic communications while in electronic storage by collecting temporarily stored location data from the iDevice Class's iPhones. *See* AC ¶¶ 58-64, 347.

Both Apple and the Mobile Industry Defendants advance four arguments why Plaintiffs' SCA claims should be dismissed for failure to state a claim, which the Court will address in turn: (1) an iPhone is not a "facility through which an electronic communication service is provided;" (2) location data on users' iPhones is not in "electronic storage;" (3) Defendants are either the electronic communications services ("ECS") providers or the intended recipient of the communications, so Plaintiffs' claims are barred by the exceptions contained in 18 U.S.C. § 2701(c)(1)-(2); and (4) Plaintiffs allege only that the iPhones communicated with Apple's servers, not that Apple accessed Plaintiffs' iPhones through unauthorized log-ins.

a. Facility

To state a claim under the SCA, Plaintiffs must allege that Defendants accessed without authorization "a facility through which an electronic communication service is provided." 18 U.S.C § 2701(a)(1). An "electronic communication service" ("ECS") is "any service which provides to users thereof the ability to send and receive wire or electronic communications." 18 U.S.C. § 2510(15). While the computer systems of an email provider, a bulletin board system, or an ISP are uncontroversial examples of facilities that provide electronic communications services to multiple users, less consensus surrounds the question presented here: whether an individual's computer, laptop, or mobile device fits the statutory definition of a "facility through which an electronic communication service is provided." The Court agrees with Defendants that it does not. Plaintiffs do not suggest that something other than their iPhones are the "facilities" allegedly accessed without authorization. *See generally* Opp'n at 10-11. Instead, Plaintiffs urge the Court to follow a number of non-binding decisions that have accepted that personal computers can be facilities. *See Chance v. Ave. A, Inc.*, 165 F. Supp. 2d 1153, 1161 (W.D. Wash. 2001); *In re Intuit Privacy Litig.*, 138 F. Supp. 2d 1272, 1275 n.3 (C.D. Cal. 2001); *Expert Janitorial, LLC v. Williams*, No. 3:09-cv-283, 2010 WL 908740, at *5 (E.D. Tenn. Mar. 12, 2010) (citing *In re Intuit*). The decisions on which Plaintiffs rely, however, provide little analysis on this point of law, instead assuming plaintiff's position to be true due to lack of argument and then ultimately ruling

on other grounds. *See, e.g., In re Intuit*, 138 F. Supp. 2d at 1275 n.3 (declining to consider defendant's argument that an individual's computer does not qualify as a "facility" under § 2701 because it was untimely raised in a reply brief).

By contrast, the courts that have taken a closer analytical look have consistently concluded that an individual's personal computer does not "provide[] an electronic communication service" simply by virtue of enabling use of electronic communication services. *See, e.g., Crowley v. Cybersource Corp.*, 166 F. Supp. 2d 1263, 1270-71 (N.D. Cal. 2001). In *Crowley*, the plaintiff made a similar argument that "computers of users of electronic communication service, as opposed to providers of electronic communication service, are considered facilities through which such service is provided." 166 F. Supp. 2d at 1271. The *Crowley* court rejected the argument that a user's computer is a "facility" under the SCA, because adopting plaintiff's construction would render other parts of the statute illogical. Another provision of the statute authorizes access to a "facility" by a provider of an electronic communication service. 18 U.S.C. § 2701(c)(1). Following Plaintiffs' logic, a service provider could grant access to a user's computer (the "facility"). "It would certainly seem odd that the provider of a communication service could grant access to one's home computer to third parties, but that would be the result of [plaintiff's] argument." *Id.* (citing 18 U.S.C. § 2701(c)(1)).

Similarly, in *Chance*, a decision that Plaintiffs themselves cite, the court first assumed that the plaintiffs' computers were "facilities" under the SCA for purposes of argument, but then quickly explained why "the subsequent implications of this rather strained interpretation of a 'facility through which an electronic communication service is provided' are fatal to [plaintiffs'] cause of action." *Chance*, 165 F. Supp. 2d at 1161. The *Chance* court explained that if an individual's personal computer is a facility under the SCA, then the web site is a "user" of the communication service provided by the individual's computer, and consequently any communication between the individual computer and the web site is a communication "of or intended for" that web site, triggering the § 2701(c)(2) exception for authorized access. Likewise here, if Plaintiffs' iPhones were the facilities, then any app downloaded by a Plaintiff would be a "user" of that service for whom the iPhone's communications are intended; any communication

between the iPhone and the app would be of or intended for that app; and the app developers would then be free under § 2701(c)(2) to authorize the disclosure of such communication to the Mobile Industry Defendants.

The Court therefore concludes that Plaintiffs fail to state a claim under the SCA because their iOS devices do not constitute "facilit[ies] through which an electronic communication service is provided."

b. Electronic Storage

Next, Defendants argue that information stored on a user's iPhone cannot be information in "electronic storage" for purposes of the SCA. To state a claim under the SCA, Plaintiffs must show not only that Defendants accessed a facility through which an electronic communication service is provided, but furthermore that Defendants "obtain[ed], alter[ed], or prevent[ed] authorized access to a wire or electronic communication while it [was] in electronic storage in such system." 18 U.S.C § 2701(a) (emphasis added). The SCA defines "electronic storage" as "(a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

The Court finds persuasive the reasoning in *In re Doubleclick, Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001). There, the court dismissed an SCA claim upon finding that the identification numbers for browser cookies the defendants installed on the plaintiffs' computers were not in "electronic storage" because they resided on the plaintiff's hard drives and thus were not in temporary electronic storage, as is required by the Act. In *In re DoubleClick*, the district court, after considering the plain language of the statute, concluded that "[the SCA] only protects electronic communications stored 'for a limited time' in the 'middle' of a transmission, i.e. when an electronic communication service temporarily stores a communication while waiting to deliver it." 154 F. Supp. 2d at 512 (quoting dictionary definitions of "temporary" and "intermediate"). The district court concluded that "[t]he cookies' long-term residence on plaintiffs' hard drives places them outside of § 2510(17)'s definition of 'electronic storage' and, hence, Title II [of the ECPA's] protection." *Id.* at 511.

The same conclusion was reached in *In re Toys R Us, Inc. Privacy Litig.*, No. 00-cv-2746, 2001 WL 34517252 (N.D. Cal. Oct. 9, 2001) (Chesney, J.), another privacy case involving cookies placed on individuals' computer hard drives. There, the plaintiffs attempted to add an allegation that the cookies were first placed in the "random access memory" ("RAM") of plaintiffs' computers, before being stored on the computers' hard drives. *Id.* at *3. Nonetheless, the court found that even if plaintiffs had pled this fact, they failed to plead that the defendant's access occurred while the cookies were in RAM, rather than on the hard drive, and thus still could not state a claim under the SCA. *Id.*

Here, the Geolocation Plaintiffs allege that Apple retrieved information from their iPhones revealing their real-time location information and that this information was necessarily only "temporarily stored" on their iPhones, because "anything other than temporary and regularly overwritten . . . data (constantly updated cell tower and WiFi network information) would quickly consume the iPhone's available memory." Opp'n at 11-12. However, Plaintiffs' own allegations in the amended complaint state that "in the /Library/Application Support/MobileSync/Backups/ folder on a user's iDevice, Apple maintains an unencrypted log of the user's movements, as often as 100 times a day, for up to a one-year period." AC ¶ 107(a). Thus, it appears that this location data resides on Plaintiffs' iPhone hard drive for up to a one-year period, which is not merely a "temporary, intermediate storage . . . incidental to the electronic transmission" of an electronic communication. Nor do Plaintiffs allege that Defendants accessed the data at a time when the data was only in temporary, intermediate storage. Thus, the Court again agrees with Defendants that Plaintiffs fail to state a claim under the SCA because they fail to allege that Defendants accessed data in "electronic storage."

c. Statutory Exceptions

Defendants argue that, even if Plaintiffs had alleged that Apple accessed a communication in "electronic storage" in a "communications facility," this conduct would fall under specific SCA exceptions for service providers or intended parties to certain communications, as provided by § 2701(c)(2). Under § 2701(c), conduct authorized by the ECS provider falls beyond the scope of § 2701(a)(1). Likewise, § 2701(a) does not apply with respect to conduct authorized "by a user of

that [electronic communications] service with respect to a communication of or intended for that user." *See* 18 U.S.C. § 2701(c).

The Court finds that the second exception under § 2701(c) applies to the Mobile Industry Defendants, but not to Apple. Here, Plaintiffs allege that Apple itself caused a log of geolocation data to be generated and stored, and that Apple designed the iPhone to collect and send this data to Apple's servers. AC ¶¶ 107(a), 114, 138. Apple, however, is neither an electronic communications service provider, nor is it a party to the electronic communication between a user's iPhone and a cellular tower or WiFi tower. Thus, the Court fails to see how Apple can avail itself of the statutory exception by creating its own, secondary communication with the iPhone. With respect to the Mobile Industry Defendants, Plaintiffs allege that when users download and install Apps on their iPhones, the Mobile Industry Defendants' software accesses personal information on those devices and sends that information to Defendants. AC ¶ 161. These allegations are highly similar to those dismissed in *In re DoubleClick* and *In re Facebook Privacy Litigation*, 791 F. Supp. 2d 705 (N.D. Cal. 2011) (Ware, J.). Thus, the App providers are akin to the web sites deemed to be "users" in *In re DoubleClick*, and the communications at issue were sent to the App providers. *See* 154 F. Supp. 2d at 508-09. Thus, because the communications were directed at the App providers, the App providers were authorized to disclose the contents of those communications to the Mobile Industry Defendants. The Mobile Industry Defendants' actions therefore fall within the statutory exception of the SCA.

d. Access Without Authorization

Defendants' final argument is that Plaintiffs fail to state a claim under the SCA because they have not alleged that Defendants "accessed" their iPhones, even if their iPhones are considered "facilities" under the SCA. Defendants again cite the *Crowley* decision, where the district court found that, notwithstanding plaintiff's conclusory allegations that the defendants "accessed" his computer, in fact "Crowley sent his information to Amazon electronically; Amazon did not gain access to his computer in order to obtain the personal information at issue." *Crowley*, 166 F. Supp. 2d at 1271.

The reasoning in *Crowley* is not as applicable to this particular argument because the nature of Plaintiffs' allegations here is rather distinct. Plaintiffs allege that when users download and install Apps on their iPhones, the Mobile Industry Defendants' software accesses personal information on those devices and supplies Defendants with details such as consumers' cellphone numbers, address books, UDIDs, and geolocation histories. AC ¶ 161. This information is not simply information that Plaintiffs themselves have voluntarily sent to the App developers, but rather information that is stored on the iPhone.

Although the Court is not persuaded that Plaintiffs have failed to allege that Defendants "accessed" their iPhones in order to obtain location data, the Court concludes that Plaintiffs have failed to allege facts sufficient to support a claim that Defendants accessed a communications facility and thereby obtained access to an electronic communication while it was in electronic storage in such system. Accordingly, Defendants' respective motions to dismiss claims one and eleven for violations of the SCA are GRANTED. The motions are granted with prejudice, for the reasons discussed in Section III.D.

2. Wiretap Act

Plaintiffs' second claim, brought by Plaintiffs Gupta and Rodimer on behalf of the Geolocation Class solely against Apple, is that Apple's conduct violated two provisions of the federal Wiretap Act, 18 U.S.C. §§ 2510-2522 (2000). *See* AC ¶¶ 230-31. The Wiretap Act generally prohibits the "interception" of "wire, oral, or electronic communications." 18 U.S.C. § 2511(1). More specifically, the Wiretap Act provides a private right of action against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication," 18 U.S.C. § 2511(1)(a), or who "intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of [the Wiretap Act]," *id.* § 2511(1)(d). *See id.* § 2520 (providing a private right of action). Plaintiffs here assert that Apple violated § 2511(1)(a) and § 2511(1)(d) by collecting Plaintiffs' precise geographic location data from Wi-fi towers, cell phone towers, and GPS data on Plaintiffs' devices, and by using that

location data to develop an expansive database of information about the geographic location of cellular towers and wireless networks throughout the United States, to Apple's benefit. AC ¶¶ 115, 137, 230-31.

Apple contends that Plaintiffs have failed to state a claim under the Wiretap Act for the following two reasons: (1) location data is not the "content" of any communication for purposes of the Wiretap Act; and (2) Apple could not have unlawfully "intercepted" the communication because it was the intended recipient of the location data. Apple MTD at 20-22.

a. Content of Communications

The Wiretap Act prohibits "interceptions" of electronic communications and defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." § 2510(4) (emphasis added). The "contents" of a communication, in turn, are defined in the statute as "any information concerning the substance, purport, or meaning of that communication." § 2510(8). "[A]ny transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce," with certain exceptions not relevant to this case, qualifies as an "electronic communication." § 2510(12).

Apple argues that information about the identities of parties to a communication and other call data is not "content" as defined by the Wiretap Act. The Court agrees. In *United States v. Reed*, 575 F.3d 900 (9th Cir. 2009), the Ninth Circuit held that data automatically generated about a telephone call, such as the call's time of origination and its duration, do not constitute "content" for purposes of the Wiretap Act's sealing provisions because such data "contains no 'information concerning the substance, purport, or meaning of [the] communication.'" *Id.* at 916 (quoting 18 U.S.C. § 2510(5)). Rather, "content" is limited to information the user intended to communicate, such as the words spoken in a phone call. *Id.* Here, the allegedly intercepted electronic communications are simply users' geolocation data. This data is generated automatically, rather than through the intent of the user, and therefore does not constitute "content" susceptible to interception.

Plaintiffs cite *In re Pharmatrak, Inc.*, 329 F.3d 9 (1st Cir. 2003), for the proposition that the definition of "contents" "encompasses personally identifiable information." Opp'n to Apple MTD at 15 (quoting *In re Pharmtrak*, 329 F.3d at 18). The Court does not find *In re Pharmatrak* persuasive because *In re Pharmatrak* cites to a footnote of a 1972 Supreme Court case discussing an outdated version of the Wiretap Act. *See Gelbard v. United States*, 408 U.S. 41, 51 n.10 (1972). The version of the Wiretap Act discussed in *Gelbard* defined "contents" as including "any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (1972). The pre-1986 definition "incude[s] all aspects of the communication itself. No aspect, including the identity of the parties, the substance of the communication between them, or the fact of the communication itself, is excluded." *Gelbard*, 408 U.S. at 51 n.10 (quoting S. Rep. No. 1097; internal quotation marks omitted). Congress, however, amended this definition in 1986 by specifically excising the phrase "information concerning the identity of the parties to such communication or the existence . . . of that communication." *See* § 2510(8) (1986). Thus, the Court concludes that under the current version of the statute, personally identifiable information that is automatically generated by the communication but that does not comprise the substance, purport, or meaning of that communication is not covered by the Wiretap Act. Because Plaintiffs allege the interception only of automatically generated geolocation data, Plaintiffs have not stated a claim for relief under the federal Wiretap Act.

b. Interception

The Court is less convinced by Apple's second argument that dismissal is warranted because Apple was the intended recipient of the Geolocation Class members' location data and therefore cannot be held liable under the Wiretap Act. Apple invokes a statutory exception to liability that protects the intended recipient of a communication. The exception provides that it is not "unlawful . . . for a person not acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is

intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or [any federal or state law]." 18 U.S.C. § 2511(2)(d).

Apple points to the assertion in the AC that "Apple designed iOS 4 to access and transmit location data from the mobile device to Apple's servers," and from that statement concludes that Apple is an intended recipient of the location data from users' mobile devices. *See* AC ¶ 142. However, this is not a fair reading of the Plaintiffs' allegations. The intended communication is between the users' iPhone and the Wi-fi and cell phone towers, and Plaintiffs appear to allege that Apple designed its operating system to intercept that communication and transmit the information to Apple's servers. Apple cannot manufacture a statutory exception through its own accused conduct, and thus the Court does not agree that § 2511(2)(d) applies.

In sum, Plaintiffs have failed to state a claim under § 2511(1)(a) or § 2511(1)(d). Accordingly, Apple's motion to dismiss count two for violation of the Wiretap Act is GRANTED. The motion is granted with prejudice, for the reasons discussed in Section III.D.

3. Invasion of Privacy Under the California Constitution

Plaintiffs, on behalf of both the Geolocation and iDevice Classes, assert that Defendants' conduct violates their right to privacy pursuant to Article I, Section 1 of the California Constitution. The California Constitution creates a privacy right that protects individuals from the invasion of their privacy not only by state actors but also by private parties. *Am. Acad. of Pediatrics v. Lungren,* 16 Cal. 4th 307 (1997); *Leonel v. Am. Airlines, Inc.*, 400 F.3d 702, 711-12 (9th Cir. 2005), *opinion amended on denial of reh'g*, 03-15890, 2005 WL 976985 (9th Cir. Apr. 28, 2005). To prove a claim under the California Constitutional right to privacy, a plaintiff must first demonstrate three elements: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) conduct by the defendant that amounts to a serious invasion of the protected privacy interest. *Hill v. Nat'l Collegiate Athletic Ass'n,* 7 Cal. 4th 1, 35-37 (1994). These elements do not constitute a categorical test, but rather serve as threshold components of a valid claim to be used to "weed out claims that involve so insignificant or de minimis an intrusion on a constitutionally protected privacy interest as not even to require an explanation or justification by the defendant." *Loder v. City of Glendale,* 14 Cal. 4th 846 (1997).

Even assuming, without deciding, that Plaintiffs have established the first two elements of a constitutional invasion of privacy claim, Plaintiffs' claim fails under the third element. "Actionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an *egregious breach* of the social norms underlying the privacy right." *Hill*, 7 Cal. 4th 1, 26, 37 (1994) (holding that rules requiring college football players to submit to drug testing were not egregious breaches of the social norms) (emphasis added). Even negligent conduct that leads to theft of highly personal information, including social security numbers, does not "approach [the] standard" of actionable conduct under the California Constitution and thus does not constitute a violation of Plaintiffs' right to privacy. *See Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1127-28 (N.D. Cal. 2008) *aff'd*, 380 F. App'x. 689 (9th Cir. 2010).

Here, the information allegedly disclosed to third parties included the unique device identifier number, personal data, and geolocation information from Plaintiffs' iDevices. Even assuming this information was transmitted without Plaintiffs' knowledge and consent, a fact disputed by Defendants, such disclosure does not constitute an egregious breach of social norms. *See, e.g. Fogelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011) ("Here, the supposed invasion of privacy essentially consisted of [Defendant] obtaining plaintiff's address without his knowledge or permission, and using it to mail him coupons and other advertisements. This conduct is not an egregious breach of social norms, but routine commercial behavior."). Accordingly, Plaintiffs have failed to establish that Defendants' conduct "amounts to a serious invasion" of the protected privacy interest. *See Hill*, 7 Cal. 4th at 26. Therefore, Defendants' motions to dismiss counts three and four for violations of California's constitutional right to privacy are GRANTED. The motions are granted with prejudice, for the reasons discussed in Section III.D.

4. Negligence

Plaintiffs, on behalf of both the Geolocation and iDevice Classes, assert a claim of negligence against Apple. The elements of negligence under California law are: "(a) a *legal duty* to use due care; (b) a *breach* of such legal duty; [and] (c) the breach as the *proximate or legal cause* of the resulting injury." *Evan F. v. Hughson United Methodist Church*, 8 Cal. App. 4th 828, 834 (1992) (italics in original). Plaintiffs argue that "Apple's breach of its duties proximately caused

Plaintiffs' highly personal information (including location information) to become exposed to it and to third parties, without Plaintiffs' consent and authorization." Opp'n at 44. Apple argues that it owes no duty to Plaintiffs because any duty was disclaimed by the App Store Terms and Conditions. *See* Apple's Mot to Dismiss at 29.

Even assuming that Apple owes an affirmative duty to protect Plaintiffs' personal data from disclosure to third parties, it is not clear how Plaintiff's have been harmed by Apple's alleged breach. As recognized by the Court's September 20 Order, in order to state a claim for negligence, Plaintiff must allege an "appreciable, nonspeculative, present injury." *See Aas v. Super. Ct.*, 24 Cal. 4th 627, 646 (2000). Moreover, in California, a consumer may not recover under a negligence theory "for purely economic loss due to disappointed expectations, unless he can demonstrate harm above and beyond a broken contractual promise." *Robinson Helicopter Co., Inc. v. Dana Corp*., 34 Cal.4th 979, 988 (2004). Purely economic damages to a plaintiff which stem from disappointed expectations from a commercial transaction must be addressed through contract law; negligence is not a viable cause of action for such claims. *Chang Bee Yang v. Sun Trust Mortg., Inc.*, No. 1:10–CV–01541 AWI, 2011 WL 902108, at *7 (E.D. Cal. Mar. 15, 2011) (citation omitted); *Robinson Helicopter*, 34 Cal. 4th at 988.

Plaintiffs allege that they were harmed "as a result of Apple's breach of its duties, which damage is separate and apart from any damage to their iPhones themselves." AC ¶ 257. Beyond this allegation, Plaintiffs have not identified what the "appreciable, nonspeculative, present injury" is. All of the allegations of harm identified in the Amended Consolidated Complaint are either too speculative to support a claim for negligence under California law, or they stem from disappointed expectations from a commercial transaction and thus do not form the basis of a negligence claim. *See, e.g.* AC ¶¶ 3, 63b, 72d, 198 (diminished and consumed iDevice resources, such as storage, battery life, and bandwidth); AC ¶¶ 4, 18, 66-67 (increased, unexpected, and unreasonable risk to the security of sensitive personal information); AC ¶¶ 29, 72c, 80-82 (disappointed expectations from commercial transaction). Because Plaintiffs have failed to establish actionable injury to state a claim for negligence, Apple's motion to dismiss is GRANTED. The motion is granted with prejudice, for the reasons discussed in Section III.D.

5. Computer Fraud and Abuse Act

Plaintiffs, on behalf of both the Geolocation and iDevice Classes, assert that the Defendants have violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. The CFAA is a federal statute that creates liability for "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access." 18 U.S.C. § 1030(a)(4).

The CFAA prohibits the following conduct, which is at issue in this lawsuit:

> "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer;
>
> "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, recklessly caus[ing] damage; or
>
> "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, caus[ing] damage and loss.

18 U.S.C. § 1030(a)(5)(A)-(C); *see also* AC ¶¶ 269-271; 284-286. A person who "intentionally accesses a computer without authorization," accesses a computer without any permission at all, while a person who "exceeds authorized access," has permission to access the computer, but accesses information on the computer that the person is not entitled to access. *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009) (quoting and interpreting 18 U.S.C. §§ 1030(a)(2) and (4)). As Plaintiffs clarified at the hearing, Plaintiffs CFAA claim rests on allegations that Defendants accessed Plaintiffs' iDevices without authorization; Plaintiffs do not allege that Defendants *exceeded* authorized access.

The CFAA is primarily a criminal statute. *AtPac, Inc. v. Aptitude Solutions, Inc.*, 730 F. Supp. 1174, 1183-84 (E.D. Cal. 2010). The CFAA authorizes a civil action only for certain enumerated conduct. *See* 18 U.S.C. § 1030(g). Specifically, Plaintiffs must allege that one of the following circumstances applies:

> (I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

> (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
>
> (III) physical injury to any person;
>
> (IV) a threat to public health or safety; [or]
>
> (V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security.

Id. at § 1030(g) & (c)(4)(A)(i)(I)(V). The only potential basis for liability in this case is pursuant to subclause (I) which requires a plaintiff to demonstrate "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000" in "economic damages." *Id.* Loss is defined as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* at § 1030(e)(11). The term "damage" means "any impairment to the integrity or availability of data, a program, a system, or information." *Id.* at § 1030(e)(8); *see Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 935 (9th Cir. 2004) ("the statutory restriction, 'limited to economic damages,' precludes damages for death, personal injury, mental distress, and the like.").

The Geolocation Class

Plaintiffs, on behalf of the Geolocation Class, assert that Apple's practice of using iDevices to retain location history files violates the above referenced provisions of the CFAA. Apple[5] first argues that Plaintiffs have failed to state a claim pursuant to the CFAA because Plaintiffs have not pled facts that establish that Apple accessed the iOS Devices without authorization. The Court agrees.

Apple rightly argues that class members "voluntarily installed" the software that caused users' iDevices to maintain, synchronize, and retain detailed, unencrypted location history files. AC ¶ 264; Apple's Mot. to Dismiss at 23. Voluntary installation of software that allegedly harmed

[5] Apple also argues that it cannot be liable under the CFAA for negligent software design. *See* 18 U.S.C. § 1030(g) ("No cause of action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware."). However, this argument is unpersuasive at the pleading stage in light of the fact that Plaintiffs allege that Apple has been *intentionally* collecting Plaintiffs' geolocation data. *See* AC ¶¶ 115, 137.

the phone was *voluntarily downloaded* by the user. Other courts in this District and elsewhere have reasoned that users would have serious difficulty pleading a CFAA violation. *See In re Apple & ATTM Antitrust Litig.*, 2010 U.S. Dist. LEXIS 98270, at *26 (N.D. Cal. July 8, 2010) ("Voluntary installation runs counter to the notion that the alleged act was a trespass and to CFAA's requirement that the alleged act was 'without authorization' as well as the CPC's requirement that the act was 'without permission.'"); *see also Specific Media*, 2011 U.S. Dist. LEXIS 50543, at *18 (on factual allegations similar to those here, noting that "it is unclear whether Specific Media can be said to have 'intentionally caus[ed] damage' to Plaintiffs' computers."). Although Apple arguably exceeded its authority when it continued to collect geolocation data from Plaintiffs after Plaintiffs had switched the Location Services setting to "off," Plaintiffs are not asserting an "exceeds authorized access" claim against Apple. Instead, Apple had authority to access the iDevice and to collect geolocation data as a result of the voluntary installation of the software (either as an update or as a native installation).

Additionally, Apple argues that the type of harm alleged with respect to this class – the cost of memory space on the class members' iPhones as a result of storing unauthorized geolocation data – is insufficient to establish the $5,000 damages minimum. In order to establish access and transmission claims pursuant to the CFAA, as the Geolocation Class attempts to here, Plaintiffs must establish that they suffered economic damage. *See Czech v. Wall Street on Demand, Inc.*, 674 F. Supp. 2d 1102, 1110 (D. Minn. 2009). A plaintiff may aggregate individual damages over the putative class to meet the damages threshold if the violation can be described as "one act." *In re Toys R Us, Inc. Privacy Litig.*, 2001 WL 34517252, *11 (N.D. Cal. 2001); *see also Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 935 (9th Cir. 2004); *see In re Doubleclick Privacy Litig.*, 154 F. Supp. 2d 497, 523 (S.D.N.Y. 2001).

Here, although Plaintiffs allege that the storage of the location histories on their iDevices consume valuable memory space, which constitutes economic damages for the purposes of the CFAA, courts have consistently rejected this argument in similar contexts. *See, e.g. Del Vecchio v. Amazon.com, Inc.*, C11-366, 2011 WL 6325910, at *4 (W.D. Wa. Dec. 1, 2011) (concluding that Plaintiffs failed to establish the $5,000 minimum damages under the CFAA where Plaintiffs had

not alleged that he or she discerned any difference whatsoever in the performance of his or her computer while visiting Defendants' site, let alone any diminution from which the Court could plausibly infer the necessary damages."); *Bose v. Interclick, Inc.*, No. 10 Civ. 9183 (DAB), 2011 U.S. Dist. LEXIS 93663, at *12-14 (S.D.N.Y. Aug. 17, 2011) (finding that Plaintiff failed to establish the economic injury required by the CFAA even though Plaintiff alleged that Defendant "impaired the functioning and diminished the value of Bose's computer in a general fashion"); *Fink v. Time Warner Cable*, No. 08 Civ. 9628, 2009 WL 2207920, *4 (S.D.N.Y. July 23, 2009) (dismissing a CFAA claim because Plaintiff only alleged that Defendant caused damage by impairing the integrity or availability of data and information, which was insufficiently factual to frame plausibly the damages element of Plaintiff's CFAA claim).

Typically, in order to establish economic damages, the consumer must establish that the Defendant intended to impair the recipient's service. *Czech*, 674 F. Supp. 2d at 1115. For example, a Defendant's unwanted text messages, alone do not cause "damage" to a consumer's cell phone by consuming limited resources. *Id.* (although the CFAA recognizes no de minimis or nominal damage exception, "the question remains whether Czech's allegations establish that her receipt of unwanted text messages necessarily constitutes 'impairment' of any magnitude."). Damage under the CFAA does not occur simply by "any use or consumption of a device's limited resources," but rather "damage" must arise from an impairment of performance "that occurs when the cumulative impact of all calls or messages at any given time exceeds the device's finite capacity so as to result in a slowdown, if not an outright 'shutdown,' of service." *Id.* at 1117; *cf. America Online, Inc. v. Nat'l Health Care Discount, Incorp.*, 121 F. Supp. 2d 1255, 1274 (N.D. Iowa 2000) ("when a large volume of [spam] causes slowdowns or diminishes the capacity of AOL to service its customers, an 'impairment' has occurred to the 'availability' of AOL's system.").

The Court further finds persuasive the reasoning employed in *AtPac, Inc. v. Aptitude Solutions, Inc.*, in which the district court narrowly construed the class of cases in which civil actions may be brought pursuant to the CFAA:

> Congress' restricting of civil actions to cases that cause the types of harm listed in 18 U.S.C. § 1030(c)(4)(A)(i) subsections (I) through (V) reemphasizes the court's conclusion that the sort of conduct alleged against [defendant] does not fall under the CFAA's

> prohibitions. "Loss" is grouped along with the harms of physical injury, threat to public health and safety, impairment of medical diagnosis or treatment, and damage to federal government computers that deal with national security and defense. It is no surprise that courts interpreting the definition of "loss" sufficient to bring a civil action have done so narrowly given the company that subsection (I) keeps. The definition of "loss" itself makes clear Congress's intent to restrict civil actions under subsection (I) to the traditional computer "hacker" scenario-where the hacker deletes information, infects computers, or crashes networks.

730 F. Supp. 2d at 1185.

Although Plaintiffs have alleged that the location files consume valuable memory space on their iDevices, Plaintiffs have not plausibly alleged that the location file *impairs* Plaintiffs' devices or interrupts service, or otherwise fits within the statutory requirements of "loss" and "economic damage" as defined by the statute. 18 U.S.C. § 1030(e)(11), (8). Thus, the Geolocation Class has failed to state a claim under the CFAA.

The iDevice Class

The Plaintiffs' claim under the CFAA on behalf of the iDevice Class suffers from a similar defect as the claims on behalf of the Geolocation Class. As the Court recognized in the September 20 Order, Plaintiffs have failed to sufficiently allege that Defendants accessed Plaintiffs' iDevices "without authorization." Where, as here, the software or "apps" that allegedly harmed the phone were voluntarily downloaded by the user, other courts in this District and elsewhere have reasoned that users would have serious difficulty pleading a CFAA violation. *See In re Apple & ATTM Antitrust Litig.*, 2010 U.S. Dist. LEXIS 98270, at *26 (N.D. Cal. July 8, 2010) ("Voluntary installation runs counter to the notion that the alleged act was a trespass and to CFAA's requirement that the alleged act was 'without authorization' as well as the CPC's requirement that the act was 'without permission.'"); *see also Specific Media*, 2011 U.S. Dist. LEXIS 50543, at *18 (on factual allegations similar to those here, noting that "it is unclear whether Specific Media can be said to have 'intentionally caus[ed] damage' to Plaintiffs' computers.").

Moreover, Plaintiffs have not established that the alleged privacy breaches performed by the Mobile Industry Defendants and allowed by Apple meet the statutory loss required for all civil actions identified above. Plaintiffs have put forth two theories that they believe demonstrate "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000" in "economic

damages." *Id.* at § 1030(g) & (c)(4)(A)(i)(I)(V). As explained below, both of these theories are insufficient to establish civil liability under the CFAA.

As explained previously in the September 20 Order, courts have tended to reject the contention that personal information – such as the information collected by the Mobile Industry Defendants – constitutes economic damages under the CFAA. *See, e.g. In re Zynga Privacy Litig.*, 2011 WL 7479170, at *3 (N.D. Cal. June 15, 2011) (rejecting the allegation that Plaintiffs' personally identifiable information constitutes a form of money or property, such that Defendant's alleged misappropriation and disclosure of that information would constitute "damage or loss . . . in excess of $5,000."); *Del Vecchio*, 2011 WL 6325910, at *3 ("While it may be theoretically possible that Plaintiffs' information could lose value as a result of its collection and use by Defendant, Plaintiffs do not plead any facts from which the Court can reasonably infer that such devaluation occurred in this case."); *Bose*, 2011 WL 4343517, at * 4 ("Only economic damages or loss can be used to meet the $5,000 threshold" and "[t]he collection of demographic information does not constitute damage to consumers or unjust enrichment to collectors.") (internal citation marks omitted).

Similarly, while Plaintiffs allege that the creation of location history files and app software components "consumed portions of the cache and/or gigabytes of memory on their devices." AC ¶ 72(d), and that the Mobile Industry Defendants conduct shortens the battery life of the iDevice, these allegations do not plausibly establish that Defendant's conduct impairs Plaintiffs' devices or service. *See, e.g. Czech*, 674 F. Supp. 2d at 1117 (rejecting CFAA under similar allegations of "impairment" to plaintiff's phone because the damage does not occur simply by "any use or consumption of a device's limited resources," but rather "damage" must arise from an impairment of performance "that occurs when the cumulative impact of all calls or messages at any given time exceeds the device's finite capacity so as to result in a slowdown, if not an outright 'shutdown,' of service."); *cf. America Online, Inc. v. Nat'l Health Care Discount, Incorp.*, 121 F. Supp. 2d 1255, 1274 (N.D. Iowa 2000) ("when a large volume of [spam] causes slowdowns or diminishes the capacity of AOL to service its customers, an 'impairment' has occurred to the 'availability' of

AOL's system."). Thus, the iDevice Class Plaintiffs have also failed to allege actionable damages pursuant to the CFAA.

In sum, Defendants' motions to dismiss the sixth and seventh causes of action for violations of the CFAA are GRANTED. The motions are granted with prejudice, for the reasons set forth in Section III.D.

6. Trespass

Plaintiffs, on behalf of both the Geolocation and iDevice Classes, assert a claim for trespass against all Defendants. Under California law, trespass to chattels "lies where an intentional interference with the possession of personal property has proximately caused injury." *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1350-51 (2003). In cases of interference with possession of personal property not amounting to conversion, "the owner has a cause of action for trespass or case [sic], and may recover only the actual damages suffered by reason of the impairment of the property or the loss of its use." *Id.* at 1351 (internal quotations and citations omitted). "[W]hile a harmless use or touching of personal property may be a technical trespass (see Rest. 2d Torts, § 217), an interference (not amounting to dispossession) is not *actionable*, under modern California and broader American law, without a showing of harm." *Id.* Even where injunctive relief is sought, "the plaintiff must ordinarily show that the defendant's wrongful acts threaten to cause *irreparable* injuries, ones that cannot be adequately compensated in damages." *Id.* at 1352 (citing 5 Witkin, Cal. Procedure (4th ed. 1997) Pleading, § 782, p. 239.).

An action for trespass arises "when [the trespass] actually did, or threatened to, interfere with the intended functioning of the system, as by *significantly reducing* its available memory and processing power." *Id.* at 1356 (emphasis added). Similarly, "intermeddling is actionable only if 'the chattel is impaired as to its condition, quality, or value or . . . the possessor is deprived of the use of the chattel for a substantial time." Plaintiffs, on behalf of the Geolocation Class, allege that Apple's creation of location history files and app software components "consumed portions of the cache and/or gigabytes of memory on their devices." Similarly, Plaintiffs, on behalf of the iDevice Class, allege that the apps provided by the Mobile Industry Defendants have taken up valuable bandwidth and storage space on their iDevices and Defendants' conduct has subsequently

shortened the battery life of the iDevice. While these allegations conceivably constitute a harm, they do not plausibly establish a significant reduction in service constituting an interference with the intended functioning of the system, which is necessary to establish a cause of action for trespass. As *Hamidi* demonstrates, trespass without harm, "by reason of the impairment of the property or the loss of use," is not actionable. *Hamidi*, 30 Cal. 4th at 1351. Accordingly, Defendants' motions to dismiss Plaintiffs' eighth cause of action for trespass are GRANTED. The motions to dismiss are granted with prejudice, for the reasons set forth in Section III.D.

7. Consumer Legal Remedies Act

Plaintiffs, on behalf of both the Geolocation Class and the iDevice Class, allege that Apple has violated the CLRA. The CLRA prohibits "unfair methods of competition and unfair or deceptive acts or practices." Cal. Civ. Code § 1770. An action may be brought under the CLRA pursuant to § 1780(a), which provides that "[any] consumer who suffers any damage as a result of the use or employment by any person of a method, act, or practice declared to be unlawful by Section 1770 may bring an action against such person." Cal. Civ. Code § 1780(a) (emphasis added). The statute proscribes a variety of conduct, including "[r]epresenting that goods or services have . . . characteristics, . . . benefits, or quantities which they do not have" (Civ. Code, § 1770, subd. (a)(5)), or "[r]epresenting that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another." *Id.*, § 1770(a)(7).

The CLRA only applies to a limited set of consumer transactions, and is not a law of "general applicability." *Ting v. AT&T*, 319 F.3d 1126, 1148 (9th Cir. 2003). For example, a violation of the CLRA may only be alleged by a consumer. *See id.*; *Von Grabe v. Sprint PCS*, 312 F. Supp. 2d 1285, 1303 (S.D. Cal. 2003). A "consumer" is defined as "an individual who seeks or acquires, by purchase or lease, any goods or services for personal, family, or household purposes." Cal. Civ. Code § 1761(d). For example, this court has previously determined that the CLRA does not apply to the sale or license of software, because software is neither a "good" nor a "service" covered by the CLRA. *See Ferrington v. McAfee*, No. 10-CV-01455-LHK, 2010 WL 3910169, at *19 (N.D. Cal. Oct. 5, 2010).

In its September 20 Order, the Court explained that Plaintiffs had failed to allege "any damage" as a result of Defendants' actions and "to the extent Plaintiffs' allegations are based solely on software, Plaintiffs do not have a claim under the CLRA." September 20 Order at 15. Plaintiffs were told that they "must remedy these deficiencies in any amended complaint." *Id.* Apple essentially argues that Plaintiffs have failed to address the previously identified deficiencies, and the CLRA claim must be dismissed because: (1) Plaintiffs have not alleged any facts establishing that Plaintiffs sustained any actual damage, (2) Plaintiffs' claim is based on the downloading of software, which is not covered by the CLRA, and (3) the CLRA applies only to the *purchase or lease* of goods or services, and Plaintiffs' claim is based on the downloading of *free* apps. *See* Apple MTD at 25-26; Apple Reply at 11-12. Apple's arguments, however, misconstrue the nature of Plaintiffs' CLRA claim in the Amended Consolidated Complaint.

As described more fully above, Plaintiffs, on behalf of the Geolocation Class, allege that Apple has stored geolocation data on users' iDevices for Apple's own benefit, and at a cost to consumers. Moreover, Plaintiffs allege that Apple continued to collect user's geolocation data even when users switched the Location Services setting to "off." Thus, Plaintiffs contend that had Apple "disclosed the true cost of the . . . geolocation features, the value of the iPhones would have been materially less than what Plaintiffs paid." *Id.* ¶ 29.

Similarly, the Amended Consolidated Complaint has clarified Plaintiffs' theory with respect to the iDevice Class. Plaintiffs allege that the availability of apps in the Apps Store is a meaningful part of Plaintiffs' decision to purchase an Apple product. Thus, Plaintiffs' theory with respect to the iDevice Class rests on representations made that Apple "takes precautions—including administrative, technical, and physical measures—to safeguard your personal information against theft, loss, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction." Plaintiffs contend that, in light of Apple's statements about protecting user privacy, Plaintiffs did not expect or consent to the tracking and collecting of their app use or otherwise personal information. *Id.* ¶ 173-74. Finally, Plaintiffs allege that as a result of Apple's failure to disclose its practices with respect to the allegedly "free apps," Plaintiffs overpaid for their iDevices. In other words "[h]ad Apple disclosed the true cost of the purportedly free Apps . . . the

value of the iPhones would have been materially less than what Plaintiffs paid." *Id.* ¶ 29. Thus, Plaintiffs have articulated a damages claim that is cognizable under the CLRA.

Moreover, the gravamen of the CLRA claim of the Geolocation Class is not that free apps downloaded by Plaintiffs were deficient, but rather that the iPhones (a "good" covered by the CLRA) purchased by the class members did not perform as promised based on a specific functionality of the device. Plaintiffs' claim thus arises out of the sale of a good, and not the downloading of free software. Similarly, Plaintiffs' CLRA claim on behalf of the iDevice class is also premised on Plaintiffs' purchase of the iDevices themselves, and not exclusively on the downloading of free apps. As explained above, Plaintiffs' theory is premised on the design of iDevices, in conjunction with the App Store and representations regarding privacy protection that led Plaintiffs to purchase the iDevices at a higher price than they otherwise would have paid. Accordingly, at the pleading stage, at least, Plaintiffs have sufficiently alleged that they are consumers under the CLRA, and their allegations relate to the purchase of goods. *See* Cal. Civ. Code § 1761(d). While these allegations may prove false, at this stage they are sufficient to state a claim under the CLRA. Apple's motion to dismiss Plaintiffs' ninth cause of action for violation of the CLRA is DENIED.

8. Unfair Competition Law

Plaintiffs, on behalf of both the Geolocation Class and the iDevice Class, allege that Apple has violated the UCL.[6] The UCL creates a cause of action for business practices that are: (1) unlawful, (2) unfair, or (3) fraudulent. Cal. Bus. & Profs. Code § 17200. Its coverage has been described as "sweeping," and its standard for wrongful business conduct is "intentionally broad." *In re First Alliance Mortg. Co.*, 471 F.3d 977, 995 (9th Cir. 2006). Each "prong" of the UCL provides a separate and distinct theory of liability. *Lozano v. AT & T Wireless Servs., Inc.*, 504 F.3d 718, 731 (9th Cir. 2007). Moreover, to assert a UCL claim, a private plaintiff needs to have "suffered injury in fact and . . . lost money or property as a result of the unfair competition." *Rubio*

[6] The Court notes that a recent Ninth Circuit decision may impact whether or not a nationwide class may be certified under California state consumer protection laws. *See Mazza v. Am. Honda Motor Co., Inc.*, 666 F.3d 581 (9th Cir. Jan. 12, 2012). The Court takes no position on this issue at this time, but notes that the parties should consider the controlling Ninth Circuit law as this case unfolds.

v. Capital One Bank, 613 F.3d 1195, 1203 (9th Cir. 2010) (quoting Cal. Bus. & Prof. Code § 17204).

a. Standing

A plaintiff must show he personally lost money or property because of his own actual and reasonable reliance on the allegedly unlawful business practices, in order to establish standing for a UCL claim. *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 330 (2011). However, there "are innumerable ways in which economic injury from unfair competition may be shown. A plaintiff may (1) surrender in a transaction more, or acquire in a transaction less, than he or she otherwise would have; (2) have a present or future property interest diminished; (3) be deprived of money or property to which he or she has a cognizable claim; or (4) be required to enter into a transaction, costing money or property, that would otherwise have been unnecessary." *Id*. at 323. In the September 20 Order, the Court dismissed Plaintiffs' UCL claim because Plaintiffs failed to allege that they lost money or property as a result of unfair competition. Specifically, the Court declined to recognize Plaintiffs' personal information as a type of "currency" or "a form of property," that was taken from Plaintiffs as a result of Defendants' business practices. *See* September 20 Order at 19-20.

In the Amended Consolidated Complaint, Plaintiffs have fleshed out their UCL claim to articulate a more traditional theory of a UCL violation. Plaintiffs, on behalf of the Geolocation Class, allege that Apple intentionally collected and stored their geographic location on the iDevices Plaintiffs had purchased despite Apple's assertion that users could disable this particular functionality. Plaintiffs contend that had Apple "disclosed the true cost of the . . . geolocation features, the value of the iPhones would have been materially less than what Plaintiffs paid." AC ¶ 29. For the Plaintiffs in the Geolocation Class, the loss of money or property is in the form of the allegedly overinflated cost of the iDevice itself as a result of the false statements regarding the geolocation features of the device. *See, e.g. Kwikset Corp.*, 51 Cal. 4th at 330 (Plaintiffs can establish UCL standing by alleging that the consumer "would not have bought the product but for" the unfair business practice or by alleging that the consumer "paid more than he or she actually valued the product."). Similarly, with respect to the iDevice Class, Plaintiffs allege that they were

induced to purchase iPhones by offering thousands of free apps, without disclosing that the apps allowed third parties to collect consumers' information. Plaintiffs allege that they overpaid for their iDevices as a result of Apple's failure to disclose its practices.

Thus, Plaintiffs have sufficiently alleged a loss of money or property as a result of the UCL violation. *See also Stearns v. Ticketmaster Corp.*, 655 F.3d 1013, 1021 (9th Cir. 2011). Because Plaintiffs have established UCL standing, the Court will address whether Plaintiffs have sufficiently alleged a claim under the UCL.

b. Unlawful Prong

The unlawful prong of the UCL prohibits "anything that can properly be called a business practice and that at the same time is forbidden by law." *Cel–Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal. 4th 163, 180 (1999) (quotation marks and citations omitted). By proscribing "any unlawful" business practice, Cal. Bus. & Profs. Code § 17200, the UCL permits injured consumers to "borrow" violations of other laws and treat them as unfair competition that is independently actionable. *Cel–Tech*, 20 Cal. 4th at 180. Plaintiffs may establish a claim under the unlawful prong of the UCL by alleging Defendants' violations of the CLRA. Thus, Plaintiffs' UCL claim survives because the CLRA claim may serve as the basis for the unlawful prong of the UCL claim.

c. Unfair Prong

The UCL also creates a cause of action for a business practice that is "unfair" even if not specifically proscribed by some other law. *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1143 (2003). In consumer cases, however, the question of what constitutes an unfair business practice appears to be unsettled. *See Lozano*, 504 F.3d at 735–36; *Boschma v. Home Loan Ctr., Inc.*, 198 Cal. App. 4th 230, 252 (2011). Some appellate state courts have applied the balancing test under S. *Bay Chevrolet v. Gen. Motors Acceptance Corp.*, 72 Cal. App. 4th 861, 886-87 (1999), which requires the Court to "weigh the utility of the defendant's conduct against the gravity of the harm to the alleged victim." *See McKell*, 142 Cal. App. 4th at 1473. Others have required a plaintiff to show that a practice violates public policy as declared by "specific constitutional, statutory or regulatory provisions" or that the practice is "immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers." *Bardin v. Daimlerchrysler*

Corp., 136 Cal. App. 4th 1255, 1260–61, 1268 (2006); *see also Lozano*, 504 F.3d at 736; *Rubio v. Capital One Bank*, 613 F.3d 1195, 1204–05 (9th Cir. 2010) (assessing plaintiff's UCL claim for unfair conduct under only the first two tests).

Regardless of what test the Court applies, the Court cannot say that at this stage Plaintiffs' claim is precluded as a matter of law. With respect to the Geolocation Class, Plaintiffs have alleged breaches of Apple's representations that it would not track consumer's whereabouts. It is possible that Apple's conduct might be useful to society, and that this benefit outweighs the harm to Plaintiffs. For example, if Apple is collecting location data to improve its own services, the benefit may outweigh the intrusion of collecting user's location data. However, at this juncture the Court cannot say that Apple's practices are not injurious to consumers, or that any benefit to consumers outweighs the harm.

Similarly, Plaintiffs have alleged "unfair" business practices with respect to the iDevice Class. Plaintiffs, on behalf of the iDevice Class, allege that Apple promotes the availability of free apps and the use of the App Store to potential purchasers of iDevices. Similarly, Apple makes affirmative representations regarding its protection of user's personal information. In contrast, according to Plaintiffs, Apple allowed third parties to collect consumers' information without their knowledge. While the benefits of Apple's conduct may ultimately outweigh the harm to consumers, this is a factual determination that cannot be made at this stage of the proceedings. Nor can the Court conclude at this stage that Apple's practices are not injurious to consumers as a matter of law. At this point, the Court declines to dismiss Plaintiffs' UCL claim under the unfair prong.

d. Fraudulent Prong

In order to state a cause of action under the fraud prong of the UCL, a plaintiff must show that members of the public are likely to be deceived. *Schnall v. Hertz Corp.*, 78 Cal. App. 4th 1144, 1167 (2000). Heightened pleading requirements under Rule 9(b) apply to UCL claims under the fraud prong. *Kearns v. Ford Motor Co.*, 567 F.3d 1125 (9th Cir. 2009). Under the federal rules, a plaintiff alleging fraud "must state with particularity the circumstances constituting fraud." Fed. R. Civ. P. 9(b). To satisfy this standard, the allegations must be "specific enough to give

defendants notice of the particular misconduct which is alleged to constitute the fraud charged so that they can defend against the charge and not just deny that they have done anything wrong." *Semegen v. Weidner*, 780 F.2d 727, 731 (9th Cir. 1985). Thus, claims sounding in fraud must allege "an account of the time, place, and specific content of the false representations as well as the identities of the parties to the misrepresentations." *Swartz v. KPMG LLP*, 476 F.3d 756, 764 (9th Cir. 2007).

Plaintiffs, on behalf of the Geolocation Class, have met their burden of pleading with particularity the basis of their UCL claim under the fraudulent prong. Plaintiffs allege that both in Apple's Terms and Conditions and in a letter to Congress, Apple has represented that consumers may opt-out of the geo-tracking feature of the iDevice by turning off the Location Services setting on the phone. AC ¶¶ 139-140. Moreover, Plaintiffs have alleged that they reasonably relied upon these representations. "While a plaintiff must show that the misrepresentation was an immediate cause of the injury-producing conduct, the plaintiff need not demonstrate it was the only cause." *In re Tobacco II Cases*, 46 Cal. 4th 298, 326–27 (2009). Here, Plaintiffs have adequately alleged that they relied upon Apple's representations regarding the ability to opt-out of geolocation tracking, in making their purchasing decisions. AC ¶¶ 76, 320, 339.

Similarly, with respect to the iDevice Class, Plaintiffs have alleged that Apple failed to disclose the "material fact that the iDevice, the App Store, the Apps, and the entire Apple ecosystem (and system of relationships with developers and [Mobile Industry Defendants]) was designed to foster the unauthorized taking of and profiting from Plaintiffs' personal information. AC ¶ 338. Moreover, Apple affirmatively asserted that it "takes precautions—including administrative, technical, and physical measures—to safeguard your personal information against theft, loss, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction." Plaintiffs contend that, in light of Apple's material omissions and affirmative statements regarding protecting user privacy, Plaintiffs did not expect or consent to the Mobile Industry Defendants' tracking and collecting their app use or personal information. *Id.* ¶ 173-74. Moreover, Plaintiffs allege that Apple's failures to disclose its practices have materially affected the value of the devices purchased. While these allegations may prove false, at this stage they are

sufficient to state a claim. Accordingly, Plaintiffs have stated a claim under the fraudulent prong of the UCL.

In sum, Apple's motion to dismiss Plaintiffs' tenth cause of action for violation of the UCL is DENIED.

9. Conversion

Plaintiffs, on behalf of the iDevice Class, allege that Apple and the Mobile Industry Defendants are liable for conversion. California law defines conversion as "any act of dominion wrongfully asserted over another's personal property in denial of or inconsistent with his rights therein. *In re Bailey*, 197 F.3d 997, 1000 (9th Cir. 1999). "The conversion of another's property without his knowledge or consent, done intentionally and without justification and excuse, to the other's injury, constitutes a willful and malicious injury within the meaning of § 523(a)(6)." *In re Bailey*, 197 F.3d at 1000 (citing *Transamerica Comm. Fin. Corp. v. Littleton*, 942 F.2d 551, 554 (9th Cir. 1994)).

To establish conversion, a plaintiff must show "ownership or right to possession of property, wrongful disposition of the property right and damages." *Kremen v. Cohen*, 337 F.3d 1024, 1029 (9th Cir. 2003). The court applies a three part test to determine whether a property right exists: "[f]irst, there must be an interest capable of precise definition; second, it must be capable of exclusive possession or control; and third, the putative owner must have established a legitimate claim to exclusivity." *Id.* at 1030; *Boon Rawd Trading Int'l Co. v. Paleewong Trading Co.*, 688 F. Supp. 2d 940, 955 (N.D. Cal. 2010).

Plaintiffs again argue that their personal information is property which is capable of exclusive possession or control. The Court, in the September 20 Order, rejected a similar argument because the weight of authority holds that a plaintiff's "personal information" does not constitute property. *Thompson v. Home Depot, Inc.*, No. 07cv1058 IEG, 2007 WL 2746603, at *3 (S.D. Cal. Sept. 18, 2007); *In re Facebook Privacy Litig.*, 2011 WL 2039995, at *6 (N.D. Cal. May 12, 2011). Plaintiffs have also failed to establish that the broad category of information referred to as "personal information" is an interest capable of precise definition. "Personal information" includes such things as a user's location, zip code, device identifier, and other data. Moreover, it is difficult

to see how this broad category of information is capable of exclusive possession or control. Therefore, Plaintiff's twelfth cause of action for conversion is DISMISSED. This dismissal is with prejudice for the reasons set forth in Section III.D.

10. Unjust Enrichment/Assumpsit/Restitution

Plaintiffs, on behalf of the iDevice Class, allege a claim against Apple and the Mobile Industry Defendants for Assumpsit and Restitution. Notwithstanding earlier cases suggesting the existence of a separate, stand-alone cause of action for unjust enrichment, the California Court of Appeals has recently clarified that "[u]njust enrichment is not a cause of action, just a restitution claim." *Hill v. Roll Int'l Corp.*, 195 Cal. App. 4th 1295, 1307 (2011); *accord Levine v. Blue Shield of Cal.*, 189 Cal. App. 4th 1117, 1138 (2010); *Melchior v. New Line Prods., Inc.*, 106 Cal. App. 4th 779, 793 (2003); *Durell v. Sharp Healthcare*, 183 Cal. App. 4th 1350, 1370 (2010). In light of this recent persuasive authority, this Court has previously determined that "there is no cause of action for unjust enrichment under California law." *Fraley v. Facebook*, 830 F. Supp. 2d 785, 2011 WL 6303898, at *23 (N.D. Cal. 2011); *accord Ferrington v. McAfee, Inc.*, No. 10–cv–01455–LHK, 2010 WL 3910169, at *17 (N.D. Cal. 2010). Other courts have similarly reached this conclusion. *See Robinson v. HSBC Bank USA*, 732 F. Supp. 2d 976, 987 (N.D. Cal. 2010) (Illston, J.) (dismissing with prejudice plaintiffs' unjust enrichment claim brought in connection with claims of misappropriation and violation of the UCL because unjust enrichment does not exist as a stand-alone cause of action); *LaCourt v. Specific Media, Inc.*, No. SACV10-1256-GW(JCGx), 2011 WL 1661532 at *8 (C.D. Cal. Apr. 28, 2011) (dismissing unjust enrichment claim because it "cannot serve as an independent cause of action"); *In re DirecTV Early Cancellation Litig.*, 738 F. Supp. 2d 1062, 1091–92 (C.D. Cal. 2010) (same). Thus, Plaintiffs' unjust enrichment claim does not properly state an independent cause of action and must be dismissed. *See Levine*, 189 Cal. App. 4th at 1138.

California courts have recognized multiple grounds for awarding restitution. *See McBride v. Boughton*, 123 Cal. App. 4th 379, 389 (2004) ("Under the law of restitution, an individual is required to make restitution if he or she is unjustly enriched at the expense of another."). Restitution may be awarded: (1) in lieu of breach of contract damages when the parties had an

express contract, but it was procured by fraud or is unenforceable or ineffective for some reason, or (2) when a Defendant obtained a benefit from the plaintiff by fraud, duress, conversion, or similar conduct." *Id.* at 388. Thus, California law recognizes that a plaintiff may elect which remedy to seek: "the plaintiff may choose not to sue in tort, but instead to seek restitution on a quasi-contract theory (an election referred to at common law as 'waiving the tort and suing in assumpsit')." *Id.* (citing *Murrish v. Indust. Indem. Co.*, 178 Cal. App. 3d 1206, 1209 (1986).

However, like unjust enrichment, California does not recognize a cause of action for restitution. *See Durell*, 183 Cal. App. 4th at 1370 (explaining that there is no cause of action in California for unjust enrichment and "[u]njust enrichment is synonymous with restitution."); *see also Robinson*, 732 F. Supp. 2d at 987 ("There is no cause of action for restitution, but there are various causes of action that give rise to restitution as a remedy."). Thus, to the extent that Plaintiffs seek to assert restitution as a stand alone cause of action, Plaintiffs' claim is dismissed. To the extent that Plaintiffs seek to elect restitution as a remedy for another tort, Plaintiffs are not entitled to restitution because they have not stated a claim for common law tort such as conversion, nor has Plaintiff established that Defendants obtained a benefit from the plaintiff by fraud or duress separate and apart from the statutory claims discussed above. Accordingly, Defendants' motion to dismiss Plaintiffs' thirteenth cause of action is GRANTED. The motions are granted with prejudice for the reasons set forth in Section III.D.

C. User Agreements

Apple also argues that all of Plaintiffs' claims against it are foreclosed by Apple's Privacy Policy and the Terms and Conditions of the iTunes Apps Store (the "Agreement"). *See* Apple's Mot. to Dismiss at 11-14, McCabe Decl. Exs. F & G. Apple makes two main arguments: (1) to the extent that Plaintiffs contest Apple's collection and transfer of user data, Apple's conduct is explicitly permitted pursuant to the terms of the Privacy Policy, and (2) the iDevice Class's claims against Apple are foreclosed because the Agreement includes a disclaimer of liability arising from third party conduct.

As explained in the September 20 Order, the Court may consider agreements between the Plaintiffs and Apple under the incorporation by reference doctrine on a motion to dismiss. *See,*

e.g., *Rubio v. Capital One Bank*, 613 F.3d 1195, 1199 (9th Cir. 2010) (reviewing disclosure agreements in a TILA action); *In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008). The Amended Consolidated Complaint refers to the Terms and Conditions for the iTunes Store ("the Agreement"). Under California contract law, "if the language [of a contract] is clear and explicit, and does not involve an absurdity," the language must govern the contract's interpretation. Cal. Civ. Code § 1638. Moreover, when a contract is written, "the intention of the parties is to be ascertained from the writing alone, if possible." Cal. Civ. Code § 1639. "[I]f reasonably practicable" a contract must be interpreted as a whole, "so as to give effect to every part, . . . each clause helping to interpret the other." Cal. Civ. Code. § 1641. However, "[i]f a contract is capable of two different reasonable interpretations, the contract is ambiguous," *Oceanside 84, Ltd. v. Fid. Fed. Bank*, 56 Cal. App. 4th 1441, 1448 (1997). Additionally, rules of construction require that the Court interpret the contract against its drafter. Cal. Civ. Code § 1654 ("In cases of uncertainty not removed by the preceeding rules, the language of a contract should be interpreted most strongly against the party who caused the uncertainty to exist.").

Based on the record before the Court, Plaintiffs have a colorable argument that the terms of the privacy agreement were ambiguous and do not necessarily foreclose the remaining claims against Apple. On the one hand, the Agreement informs users that Apple may collect "non-personal information" including "zip code, area code, unique device identifier, [and] location" and the Agreement authorizes Apple to "collect, use, transfer, and disclose non-personal information for any purpose." However, Apple also limits how it may utilize users' "personal information" which it defines as "data that can be used to uniquely identify or contact a single person." It does appear that there is some ambiguity as to whether the information collected by Apple, including the user's unique device identifier, is personal information under the terms of the Agreement, and thus whether Apple's collection and use of the information is consistent with the Agreement's terms.

Additionally, to the extent that Apple argues that it has no duty to review or evaluate apps and that it has disclaimed any liability arising from the actions of third parties, this argument both ignores contradictory statements made by Apple itself, and the allegations asserted by Plaintiffs regarding Apple's own conduct with respect to the alleged privacy violations. For one, it is not

clear that Apple disclaimed all responsibility for privacy violations because, while Apple claimed not to have any liability or responsibility for any third party materials, websites or services, Apple also made affirmative representations that it takes precautions to protect consumer privacy. Additionally, Plaintiffs' allegations go beyond asserting that Apple had a duty to review or police third party apps. Instead, Plaintiffs allege Apple was responsible for providing user's information to third parties. AC ¶¶ 25, 30. Plaintiffs allege that Apple is independently liable for any statutory violations that have occurred. At the motion to dismiss stage, then, the Court is not prepared to rule that the Agreement establishes an absolute bar to Plaintiffs' claims.

D. Leave to Amend

In order to determine whether leave to amend should be granted, the Court must consider "undue delay, bad faith or dilatory motive on the part of the movant, repeated failure to cure deficiencies by amendments previously allowed, undue prejudice to the opposing party by virtue of allowance of the amendment, [and] futility of amendment, etc.'" *Eminence Capital, LLC v. Aspeon, Inc.*, 316 F.3d 1048, 1051-52 (9th Cir. 2003) (quoting *Foman v. Davis*, 371 U.S. 178, 182 (1962)).

This is the second order that the Court has issued dismissing several of Plaintiffs' claims for relief. After the September 20 Order outlining deficiencies in the Consolidated Complaint, Plaintiffs were granted leave to amend the complaint in order to address the deficiencies. Plaintiffs reasserted several claims in the Amended Consolidated Complaint that had been asserted in the first Consolidated Complaint. Thus, for many of Plaintiffs' claims, including claims for trespass, negligence, violation of the CFAA, and restitution/assumpsit, this is the second time these claims are being dismissed. Therefore, the Court finds that amendment of these claims is futile. *See Nordyke v. King*, 644 F.3d 776, 788 n.12 (9th Cir. 2011) (leave to amend need not be granted where doing so would be an exercise in futility).

In addition, Plaintiffs included for the first time violations of the SCA, the Wiretap Act, the California Constitution, and a claim for conversion in the Amended Consolidated Complaint. Although these claims were not initially raised in the Consolidated Complaint, the Court nonetheless finds that amendment would be futile as to these claims as well. As explained above,

Plaintiffs' claims fail not based on a deficiency in pleading, but rather because the theories regarding how Defendants' practices constitute actionable conduct are defective. For example, it does not appear that additional allegations will establish that the iPhone is a "facility" under the SCA or that personal data is "content" pursuant to the Wiretap Act. Similarly, it is unlikely that Plaintiffs can amend their allegations to establish the type of egregious breach of social norms required to establish a constitutional privacy claim, or how "personal information" constitutes a property interest for the purposes of stating a conversion claim. Accordingly, Plaintiffs will not be granted leave to amend to cure the deficiencies in their Amended Consolidated Complaint.

III. CONCLUSION

For the reasons stated above, the Court DENIES Defendants' motions to dismiss pursuant to Rule 12(b)(1). However, the Court GRANTS the Mobile Industry Defendants' motion to dismiss pursuant to Rule 12(b)(6) in its entirety, without leave to amend. The Court GRANTS in part, and DENIES in part, Apple's motion to dismiss pursuant to Rule 12(b)(6). Specifically, Plaintiffs' claims against Apple for violations of the Stored Communications Act, violations of the Wiretap Act, violations of the California Constitutional right to privacy, negligence, violations of the Computer Fraud and Abuse Act, trespass, conversion, and unjust enrichment/assumpsit/ restitution are dismissed without leave to amend. The claims against Apple for violations of the UCL and CLRA survive the motion to dismiss.

IT IS SO ORDERED.

Dated: June 12, 2012

Lucy H. Koh

LUCY H. KOH
United States District Judge